

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

DETRINA SOLOMON, on behalf of)
herself and all others similarly situated,)

Plaintiff,)

v.)

1:22-CV-526

ECL GROUP, LLC,)

Defendant.)

MEMORANDUM OPINION AND ORDER

Catherine C. Eagles, District Judge.

After receiving notice from her eye care clinic that her personal information had been accessed by data thieves, the plaintiff Detrina Solomon noticed an increase in spam texts, calls, and emails. Believing this increase to be associated with the data breach and concerned about the potential future threat of identity theft, Ms. Solomon changed her phone numbers and the passwords to her digital and electronic accounts. She then brought this class action lawsuit against the defendant, ECL Group, LLC, the entity that electronically manages access to her personal information on behalf of the clinic and whose data was breached.

Because Ms. Solomon alleges facts sufficient to plausibly establish standing and ECL's remaining arguments are better presented and evaluated on a more developed factual record, the defendant's motion to dismiss will be denied. And because this case raises common issues with four other cases recently consolidated for discovery, the plaintiff's motion to consolidate will be granted in part for discovery purposes.

I. Overview of Factual Allegations and Causes of Action

ECL provides medical records platforms and patient management software to eye care clinics across the country. Doc. 1 at ¶ 15. ECL provides services to more than 9,000 physicians. *Id.* Its technology is cloud-based with data stored on servers where it is accessed by clinic staff. *Id.*

As a result, ECL maintains and controls sensitive patient information. *Id.* at ¶ 16. Patients provide personal health information and identifying information to their clinics and physicians who store and manage that data through ECL. *Id.* This includes dates of birth, health insurance information, Social Security numbers, and health care information. *Id.* at ¶ 27. Ms. Solomon estimates that because ECL serves thousands of clinics, it likely controls access to the patient information of “hundreds of thousands of individuals.” *Id.* at ¶ 16.

Ms. Solomon provided her personal information to Eye Mart, an eyecare clinic in Texas that uses ECL’s services. *Id.* at ¶¶ 1, 13. ECL controlled and managed access to Ms. Solomon’s information on behalf of Eye Mart. *Id.* at ¶ 1.

“On or around December 4, 2021, a malicious actor gained unauthorized access” to ECL’s “databases, system configuration files, and data.” *Id.* at ¶ 26. The actor also gained access to the personal information of ECL’s clients’ patients, *id.*, and then “viewed, copied and exfiltrated” much of this information.¹ *Id.* at ¶ 27.

¹ According to one dictionary, to “exfiltrate” means to furtively remove. *Exfiltrate*, MERRIAM-WEBSTER.COM, <https://www.merriam-webster.com/dictionary/exfiltrate> (last visited Jan. 24, 2023). In the context of a data breach, it means to steal sensitive data. *Id.*

Ms. Solomon “received a notice that her information was impacted by” the breach. *See id.* at ¶ 13. After receiving this notice, Ms. Solomon experienced “an increase in spam texts, spam calls, and spam emails.” *Id.* The phone calls were so frequent that Ms. Solomon changed phone numbers. *Id.* She also “changed passwords on her personal accounts to prevent any identity theft.” *Id.*

Ms. Solomon brings claims for damages based on negligence, negligence *per se*, and unfair and deceptive trade practices under N.C. Gen. Stat. § 75-1.1. She also seeks a declaratory judgment that ECL owed and continues to owe legal duties to her and other proposed class members. She asserts federal jurisdiction under 28 U.S.C. § 1332(d), the Class Action Fairness Act.

II. Analysis

A. Standing

ECL contends that Ms. Solomon’s complaint should be dismissed because she fails to allege facts that plausibly show she has standing to sue. Doc. 12 at 7. This is a facial challenge to standing, so all well-pleaded facts in the complaint are accepted as true and construed in the light most favorable to Ms. Solomon. *See Wikimedia Found. v. Nat’l Sec. Agency*, 857 F.3d 193, 208 (4th Cir. 2017).

“The doctrine of standing is an integral component of the case or controversy requirement” of federal jurisdiction. *Miller v. Brown*, 462 F.3d 312, 316 (4th Cir. 2006). “The party invoking federal jurisdiction bears the burden of establishing” standing. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992). The party “must demonstrate

standing for each claim” and “for each form of relief” it seeks. *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2208 (2021).

Standing under Article III has three elements: (1) “the plaintiff must have suffered an injury in fact,” (2) the injury must be “fairly traceable” to the defendant, and (3) “it must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.” *Lujan*, 504 U.S. at 560–61 (cleaned up). Injury in fact is the “invasion of a legally protected interest which is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical.” *Lujan*, 504 U.S. at 560 (cleaned up). “For an injury to be particularized, it must affect the plaintiff in a personal and individual way.” *Spokeo, Inc. v. Robins*, 578 U.S. 330, 339 (2016) (cleaned up). “A concrete injury must be *de facto*; that is, it must actually exist.” *Id.* at 340 (cleaned up). “[I]ntangible harms can also be concrete.” *TransUnion*, 141 S. Ct. at 2204 (discussing how reputational harms, disclosure of private information, and abridgement of free speech qualify as concrete harms). Two recent Fourth Circuit cases provide helpful guidance in evaluating injury and traceability in a data breach case.

In *Beck v. McDonald*, the court considered two consolidated appeals brought by plaintiffs who sued a medical center after two data breaches compromised their personal information. 848 F.3d 262, 266–67 (4th Cir. 2017). In one underlying case, a laptop computer containing unencrypted patient information was either lost or stolen. *Id.* at 267. In the other, “four boxes of pathology reports headed for long-term storage” and containing personal information “had been misplaced or stolen.” *Id.* at 268. In both

cases, the plaintiffs alleged injury in fact based on an increased risk of identity theft, and the district courts dismissed the claims for lack of standing. *Id.* at 267–69.

The Fourth Circuit affirmed, agreeing that the harms alleged were too speculative to establish standing because they required the court to engage with and credit an “attenuated chain of possibilities.” *Id.* at 275 (quoting *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 410 (2013)). To find harm, the court would have to assume “that the thief targeted the stolen items for the personal information they contained” and that the thief would “then select, from thousands of others, the personal information of the named plaintiffs and attempt successfully to use that information to steal their identities.” *Beck*, 848 F.3d at 275. This chain of possibilities was not sufficient to confer standing, especially since there was no indication that the information had been stolen for the purpose of identity theft or that any plaintiff was the victim of identity theft. *Id.*

The next year, the Fourth Circuit considered *Hutton v. Nat’l Bd. of Exam’rs in Optometry, Inc.*, involving three optometrist-plaintiffs whose personal information was allegedly stolen when thieves stole data from the defendant, the National Board of Examiners in Optometry, Inc. 892 F.3d 613, 616 (4th Cir. 2018). Despite allegations that after the data breach unauthorized persons opened credit cards in the plaintiffs’ names, that their identities had thus been stolen, and that they had spent time and money on mitigation, the district court dismissed the claims for lack of standing. *Id.* at 617–18.

The Fourth Circuit distinguished the case from *Beck* and reversed, explaining that “[i]n *Beck*, the plaintiffs alleged only a threat of future injury in the data breach context where a laptop and boxes” containing personal information “had been stolen, but the

information contained therein had not been misused.” *Id.* at 621–22. In contrast, the plaintiffs in *Hutton* “allege[d] that they ha[d] already suffered actual harm in the form of identity theft and credit card fraud.” *Id.* at 622. They had thus “been concretely injured by the data breach” because someone used or attempted to use their information to open credit cards without their knowledge. *Id.* Unlike in *Beck*, this harm was not speculative and was sufficient to allege injury in fact. *Id.*

This case is more like *Hutton* than *Beck*. Unlike in *Beck* where a laptop was either stolen or lost and four boxes of pathology reports were missing, *Beck*, 848 F.3d at 267–69, 274–75, thieves here targeted personal information in a massive and deliberate act, giving rise to an easy inference that the thieves intended to misuse the personal information they stole. There may be many reasons unrelated to identity theft why someone might steal a laptop, such as obtaining the laptop itself, and it is not uncommon for old boxes of documents to be lost or misplaced. But one is hard pressed to think of a reason why data thieves would engage in a large-scale and sophisticated operation to steal electronic data containing personal information and only personal information other than to misuse it, either by identity theft or perhaps as part of a blackmail or ransomware type scheme. *See Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015) (“Why else would hackers break into a store’s database and steal consumers’ private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers’ identities.”).

As in *Hutton*, Ms. Solomon has alleged that thieves targeted and stole personal information to misuse it. Unlike the plaintiffs in *Beck*, there are no other equally likely

reasons for the theft and no possibility that the information was simply misplaced. The Fourth Circuit in *Beck* implied that such allegations would be sufficient to establish standing, *see Beck*, 848 F.3d at 274, and other district courts have found such allegations of targeted data theft to be sufficient to establish standing. *See In re Marriott Int’l, Inc. Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 459 (D. Md. 2020) (finding standing when the defendant “disclosed that it was the target of” a cyberattack and distinguishing the case from *Beck* “where there were no allegations of targeting”); *Stamat v. Grandizio Wilkins Little & Matthews, LLP*, No. 22-CV-747, 2022 WL 3919685, at *6 (D. Md. Aug. 31, 2022) (“[C]ourts have permitted a plaintiff to establish standing where the [personal identifying information] was the specific target of the attack.”).

Like the plaintiffs in *Hutton*, Ms. Solomon also alleges actual misuse of her information; at some unidentified time after receiving notice of the data breach, she “noticed an increase in spam texts, spam calls, and spam emails.” Doc. 1 at ¶ 13. The spam calls were so frequent that Ms. Solomon changed her phone numbers. *Id.* This injury is sufficient to satisfy Article III standing. *See Krakauer v. Dish Network, L.L.C.*, 925 F.3d 643, 653 (4th Cir. 2019); *Garey v. James S. Farrin, P.C.*, 35 F.4th 917, 921–22 (4th Cir. 2022); *McCreary v. Filters Fast LLC*, No. 20-CV-595, 2021 WL 3044228, at *4–5 (W.D.N.C. July 19, 2021).

Accepting the allegations in the complaint as true, the injury is “fairly traceable” to ECL. *See Lujan*, 504 U.S. at 560. The “fairly traceable” standard is not the same as the tort causation standard. *Friends of the Earth, Inc. v. Gaston Copper Recycling Corp.*, 204 F.3d 149, 161 (4th Cir. 2000). Instead, “[i]t must simply be plausible that” the data

breach “was the cause” of Ms. Solomon’s spam. *See Bank of La. v. Marriott Int’l, Inc.*, 438 F. Supp. 3d 433, 441 (D. Md. 2020). Ms. Solomon has established standing to the extent required at this stage.

ECL challenges the redressability requirement only to the extent Ms. Solomon seeks prospective relief. Doc. 12 at 11. “A plaintiff can satisfy the injury-in-fact requirement for prospective relief either by demonstrating a sufficiently imminent injury in fact or by demonstrating an ongoing injury.” *Garey*, 35 F.4th at 922 (cleaned up).

Accepting the allegations in the complaint as true, Ms. Solomon has established a substantial risk of future injury. She alleges the targeted theft of personal information and the misuse of that information; her fear of future injury is not just speculative. *See In re Marriott Int’l, Inc.*, 440 F. Supp. 3d at 460 (“The allegations about the targeting of personal information in the cyberattack and the allegations of identity theft by other plaintiffs whose personal information was stolen makes the threatened injury sufficiently imminent.”); *Desue v. 20/20 Eye Care Network, Inc.*, No. 21-CV-61275, 2022 WL 796367, at *5 (S.D. Fla. Mar. 15, 2022). She provides facts that plausibly allege a significant risk ECL will again be targeted by data thieves, *see, e.g.*, Doc. 1 at ¶ 24 (ECL did not employ reasonable data security measures after the breach), *id.* at ¶ 118 (allegations about defects in ECL’s systems and platforms), and alleges that ECL continues to store her personal information. *Id.* at ¶ 128.

B. Failure to State a Claim

ECL argues that Texas law governs Ms. Solomon’s claims and that under Texas law the claims all fail. In a diversity case, a federal district court applies the choice of

law rules of the state in which it sits. *Perini/Tompkins Joint Venture v. Ace Am. Ins. Co.*, 738 F.3d 95, 100 (4th Cir. 2013). In tort and “tort-like” actions, North Carolina follows the rule of *lex loci*, applying the law of the state where the injury occurred. *SciGrip, Inc. v. Osaе*, 373 N.C. 409, 420, 838 S.E.2d 334, 343 (2020); *Boudreau v. Baughman*, 322 N.C. 331, 335, 368 S.E.2d 849, 854 (1988) (applying law of the place where the injury occurred in a negligence case); *Harco Nat’l Ins. Co. v. Grant Thornton LLP*, 206 N.C. App. 687, 692, 698 S.E.2d 719, 722–23 (2010) (citing *Boudreau*, 368 S.E.2d at 853–54). This is ordinarily “the state where the last event necessary to make the actor liable or the last event required to constitute the tort takes place.” *SciGrip*, 838 S.E.2d at 343 (cleaned up).

Each cause of action must be evaluated separately to determine what the alleged injury is and where it allegedly occurred. *Boudreau*, 368 S.E.2d at 853–54 (analyzing causes of action separately for conflict of law purposes). This may be, but is not necessarily, the plaintiff’s place of residence; the *lex loci* test “requires application of the law of the state where the plaintiff has actually suffered harm.” *Harco*, 698 S.E.2d at 726 (applying the *lex loci* test to a misappropriation of trade secrets claim and rejecting the defendant’s argument that the law where the plaintiff resided was automatically the law that applied).

In a data breach case applying the *lex loci* test under similar if not identical South Carolina law at the motion to dismiss stage, the United States District Court for the District of South Carolina has concluded that as to various negligence claims, the injury occurs when the data is stolen. *In re Blackbaud, Inc., Customer Data Breach Litig.*, 567

F. Supp. 3d 667, 675 (D.S.C. 2021). The court applied the law of the state where the defendant was headquartered “because the place of the breach cannot be determined without further discovery and South Carolina is the only Blackbaud location specifically enumerated in the record.” *Id.* at 676.

So too here. For purposes of the motion to dismiss, the Court will apply North Carolina law. *See, e.g.*, Doc. 1 at ¶¶ 10–11, 14 (detailing ECL’s operations in North Carolina). A more definitive resolution of the choice of law question is deferred until “after the parties have developed the factual evidence through the process of discovery,” *Clean Earth of Md., Inc. v. Total Safety, Inc.*, No. 10-CV-119, 2011 WL 1627995, *4 (N.D.W. Va. Apr. 28, 2011), and with briefing that addresses more specifically where the injury ascribed to each cause of action arose. *See, e.g., In re Blackbaud, Inc.*, 567 F. Supp. 3d at 675 n.5 (collecting cases supporting this approach).

ECL argues that Ms. Solomon fails to state any valid claim for relief under North Carolina law. But a plaintiff is not required to prove her case in the complaint. *See Robertson v. Sea Pines Real Est. Cos.*, 679 F.3d 278, 291 (4th Cir. 2012) (“*Iqbal* and *Twombly* do not require a plaintiff to prove his case in the complaint.”). Ms. Solomon has met the minimal standard of plausibility for her negligence, negligence *per se*, and Chapter 75 claims, and any weaknesses of those claims will be better evaluated on a factual record.

C. Motion to Consolidate

Ms. Solomon moves to consolidate this case with four related actions that were recently consolidated for discovery: (1) Farley, et al. v. Eye Care Leaders Holdings,

LLC, No. 22-CV-468; (2) Forrester, et al. v. Eye Care Leaders Holdings, LLC, No. 22-CV-503; (3) Sandvig, et al. v. Eye Care Leaders Holdings, LLC, No. 22-CV-502; and (4) Byers, et al. v. ECL Group, LLC, No. 22-CV-607. Doc. 20; *see also Farley v. Eye Care Leaders Holdings, LLC*, No. 22-CV-468, Doc. 34.

This case and the other cases are all brought by individuals whose personal information allegedly safeguarded by ECL was compromised by data breaches in 2021. There are overarching common questions of law and fact in these cases, and consolidation for discovery purposes poses no real risks of prejudice or confusion.

District courts have broad discretion to consolidate actions if the actions “involve a common question of law or fact.” Fed. R. Civ. P. 42(a); *see A/S J. Ludwig Mowinckles Rederi v. Tidewater Const. Co.*, 559 F.2d 928, 933 (4th Cir. 1977); *Campbell v. Bos. Sci. Corp.*, 882 F.3d 70, 74 (4th Cir. 2018) (listing relevant factors to consider). Because these cases raise many common issues, and consistent with the order consolidating the other cases, *Farley et al. v. Eye Care Leaders Holdings, LLC*, No. 22-CV-468, Doc. 34, the motion to consolidate will be granted in part and this case will be consolidated with the others for purposes of discovery. The Court will decide later if consolidation for trial is appropriate.

For now, the cases shall remain separate for trial. The case caption for each separate case should be included on all consolidated filings. Consolidated filings shall only be made on the ECF docket for the lead case, *Farley et al. v. Eye Care Leaders Holdings, LLC*, No. 22-CV-468. Counsel shall discuss with the Magistrate Judge

procedures to ensure that duplicative motions are not filed in each case when a consolidated motion is more efficient.

III. Conclusion

Ms. Solomon alleges targeted data theft of her personal information as well as actual misuse of that information to send her excessive spam messages. These allegations are sufficient to support standing. And ECL's arguments on choice of law and otherwise are better evaluated on a more fully developed record. ECL's motion to dismiss will be denied.

Because this case raises common questions with four other cases that were recently consolidated, Ms. Solomon's motion to consolidate the cases is granted in part. The cases will be consolidated for discovery.

It is **ORDERED** that:

1. The defendant's motion to dismiss, Doc. 11, is **DENIED**.
2. The plaintiff's motion to consolidate, Doc. 20, is **GRANTED in part**.

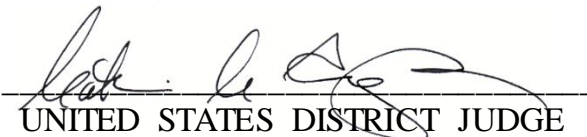
This case is consolidated with Farley, et al. v. Eye Care Leaders Holdings, LLC, No. 22-CV-468, Forrester, et al. v. Eye Care Leaders Holdings, LLC, No. 22-CV-503, Sandvig, et al. v. Eye Care Leaders Holdings, LLC, No. 22-CV-502, and Byers, et al. v. ECL Group, LLC, No. 22-CV-607, for the purposes of discovery.

3. The parties **SHALL** caption their consolidated filings with all the case names and numbers. Consolidated filings shall only be made on the ECF docket for the lead case, Farley et al. v. Eye Care Leaders

Holdings, LLC, No. 22-CV-468. The Clerk's office will enter a docket entry on that docket, noting that the case has been consolidated with No. 22-CV-526 for purposes of discovery.

4. At the initial pretrial conference, counsel **SHALL** discuss with the Magistrate Judge procedures to ensure that duplicative motions are not filed in each case when a consolidated motion is more efficient.

This the 30th day of January, 2023.


UNITED STATES DISTRICT JUDGE